सावधान रहें, जागरूक बने

BE(A)WARE

वित्तीय धोखेबाजों की कार्यप्रणाली पर बुकलेट

A BOOKLET ON MODUS OPERANDI OF FINANCIAL FRAUDSTERS

OFFICE OF THE RBI OMBUDSMAN (MUMBAI-II)
MAHARASHTRA AND GOA


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

विषय वस्तु

आमुख

हाल के वर्षों में भुगतान के डिजिटल साधनों/तरीकों के प्रयोग में काफी वृद्धि हुई है। इससे न केवल ग्राहकों की सुलभता बढ़ी है, अपितु वित्तीय समावेशन के राष्ट्रीय उद्देश्य को काफी हद तक हासिल करने में मददगार साबित हुआ है। जैसे ही वित्तीय लेनदेन करने में आसानी हुई, खुदरा वित्तीय लेनदेनों की धोखाधड़ी के मामलों में वृद्धि हुई। धोखेबाज आम/जनसाधारण एवं मासूम/भोले-भाले लोगों, के मेहनत से कमाए गए धन को ठगने/हड़पने के लिए नवीनतम तरीकों का उपयोग कर रहे हैं, खासकर नए लोगों/सहभागियों को जो टेक्नो – फाइनेंशियल इको सिस्टम से भलीभांति : परिचित नहीं हैं।

इस बुकलेट के संकलन का, एकमात्र उद्देश्य यह है कि वास्तविक मूल्य की अधिकतम व्यावहारिक जानकारी को इसमें समाहित करना है, विशेषत: उनके लिए जिन्हें वित्तीय लेनदेन का अनुभव नहीं है। यह केवल विभिन्न स्त्रोतों से यादृच्छिक रूप से एकत्रित घटनाओं का संकलन मात्र नहीं है, अपितु बैंकिंग लोकपाल के कार्यालय में प्राप्त विभिन्न प्रकार की शिकायतों का बड़ी सावधानी से संकलित किया हुआ दस्तावेज़ है। यह बुकलेट धोखेबाज लोगों की कार्यप्रणाली के बारे में आम जनता में जागरूकता पैदा करने का प्रयास मात्र है, इसके अतिरिक्त वित्तीय लेनदेन के समय बरती जाने वाली सावधानियों के विषय में भी कुछ जानकारी प्रदान करती है। यह बुकलेट व्यक्तिगत जानकारी को सुरक्षित, अनजान कॉल / ईमेल से सावधान रहने, वित्तीय लेनदेन करते समय समुचित सावधानी बरतने, समय – समय पर सुरक्षित निजी जानकारी/पासवर्ड को बदलने पर ज़ोर देती है। इसलिए इसका शीर्षक अंग्रेजी में BE(A)WARE है इसीलिए हिन्दी में इसे कहा जा सकता है – सावधान रहें और जागरूक बनें।

यह पुस्तिका/बुकलेट आम जनता में जागरूकता पैदा करने के लिए इस कार्यालय द्वारा की गई पहल का एक हिस्सा है।

धोखाधड़ीपूर्ण लेनदेन की कार्यप्रणाली और उसके विरुद्ध बरती जाने वाली सावधानियाँ - बैंक

1. फिशिंग संबंधी लिंक

कार्यप्रणाली

- धोखेबाज एक तृतीय पक्षकार (थर्ड पार्टी) वेबसाइट बनाते हैं, जो कि वास्तविक वेबसाइट्स की तरह ही प्रतीत होती है, जैसे कि बैंक की वेबसाइट्स या ई-कॉमर्स वेबसाइट्स या सर्च इंजन इत्यादि।
- धोखेबाजों द्वारा सामान्यत: ये लिंक एसएमएस / सोशल मीडिया / ईमेल / इंसटेंट मैसेजिंग आदि के द्वारा भेजे जाते हैं।
- अधिकांश समय, ग्राहक पूरे / विस्तृत यूआरएल को जाँचे बिना, सिर्फ एक ही झलक में और लिंक को क्लिक करके सुरक्षित निजी जानकारी को प्रविष्ट करते हैं।
- यह लिंक वेबसाइटों के प्रमाणिक दिखने वाले नामों जैसे दिखाई देतें हैं, किंतु , वास्तव में, ग्राहक फिशिंग वेबसाइट्स की ओर पुनर्निर्देशित (रिडायरेक्ट) हो जाता है।

- जब ग्राहक इन वेबसाइट्स पर अपनी सुरक्षित निजी जानकारी डालते हैं, तो उसको हथिया लिया जाता है और धोखेबाजों द्वारा प्रयोग में लाया जाता है।

सावधानी

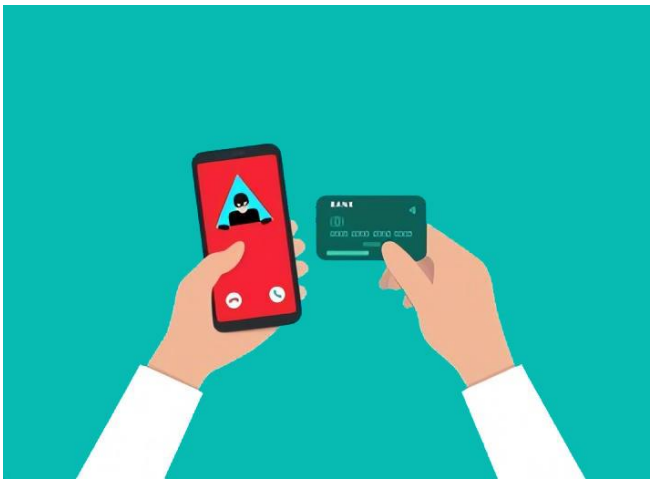
अनजान लिंक को क्लिक नहीं करना चाहिए तथा एसएमएस / ईमेल को तत्काल ही डिलीट कर देना चाहिए ताकि भविष्य में उनकी पहुँच से बचा जा सके। वेबसाइट्स के सत्यापन के समय सावधानी बरतनी चाहिए, विशेषत: जब वित्तीय जानकारी प्रविष्ट करनी हो।

2. टेलीफोन पर छद्म कॉल (विशिंग)

कार्यप्रणाली

- बहुरूपिए व्यक्ति बैंकर्स / कंपनी कार्यपालक / बीमा एजेंट / सरकारी अधिकारी इत्यादि के रूप में ग्राहक से टेलीफोन कॉल / सोशल मीडिया / के माध्यम से संपर्क करते हैं और विश्वास कायम करने के लिए नाम या जन्म तिथि जैसे कुछ विवरण साझा करते हुए सुरक्षित जानकारी की पुष्टि कराते हैं।

- कुछ मामलों में, बहुरूपिए व्यक्ति लेनदेन को ब्लॉक करने के लिए आवश्यक ब्योरे, दंड को रोकने हेतु अपेक्षित भुगतान आकर्षक छूट प्राप्त करने इत्यादि हेतु आकस्मिकता / आपातकाल बताकर ग्राहक को अत्यावश्यक / तत्काल सूचनाएँ साझा करने के लिए दबाव डालते हैं / अपनी चाल में फँसाते हैं। बाद में इन जानकारियों का इस्तेमाल ग्राहकों के साथ धोखाधड़ी करने के लिए किया जाता है।



सावधानी

बैंक अधिकारी / वित्तीय संस्थाएं / कोई अन्य वास्तविक संस्था ग्राहक से गोपनीय जानकारी जैसे यूज़रनेम / पासवर्ड / कार्ड विवरण / सीवीवी / ओटीपी इत्यादि साझा करने के लिए कभी नहीं कहते हैं।

3. ऑनलाइन बिक्री प्लेटफॉर्म के प्रयोग से धोखाधड़ी

कार्यप्रणाली

- धोखेबाज ऑनलाइन बिक्री प्लेटफॉर्म पर खरीददार होने का बहाना करके और आपके उत्पाद में रुचि दर्शाते हैं।
- धन आपको भुगतान करने के बजाए, वे यूपीआई एप के माध्यम से "धन अनुरोध" (Request money) विकल्प का प्रयोग करते हैं और आपके बैंक खाते से पैसा ऐंठने के लिए अनुरोध को अनुमोदित करने हेतु जोर देते हैं।

सावधानी

- ऑनलाइन उत्पादों हेतु वित्तीय लेनदेन के समय सावधानी बरतनी चाहिए।
- हमेशा याद रखें कि धन प्राप्त करने के लिए कहीं भी अपना पिन / पासवर्ड डालने की आवश्यकता नहीं होती है।
- यदि यूपीआई या कोई अन्य एप के माध्यम से आपसे लेनदेन पूरा करने के लिए आपका पिन डालने के लिए निर्देश देते हैं, तो इसका मतलब है कि आप धन प्राप्त करने की जगह धन भेजने की ओर अग्रसर हो रहे हैं।

4. अनजान / गैर सत्यापित मोबाइल एप्स के कारण धोखाधड़ी

कार्यप्रणाली

- जब आप अनजान / गैर सत्यापित मोबाइल एप्स डाउनलोड करते हैं तो धोखेबाज़ को आपके मोबाइल डिवाइस / लेपटॉप / डेस्कटॉप तक पहुँच मिल जाती है।
- इन एप्लीकेशन के लिंक सामान्यत: एसएमएस/सोशल मीडिया / इंसटेंट मेसेंजर इत्यादि के माध्यम से साझा किए जाते हैं। ये लिंक प्रमाणिक दिखने वाले नामों जैसे ही लगते हैं परंतु वास्तव में ग्राहक को अनजान एप्लिकेशन को डाऊनलोड करने के लिए पुनर्निर्देशित (री-डाइरेक्ट) करते है।
- जब एक बार नकली एप्लिकेशन डाउनलोड हो जाती है, तो धोखेबाज डिवाइस तक पूर्ण पहुँच हासिल कर सकते हैं।

सावधानी

अनजान / गैर सत्यापित स्त्रोतों से कभी भी एप्लिकेशन डाऊनलोड नहीं करें।

5. एटीएम कार्ड स्किमिंग (डाटा चोरी करने की डिवाइस)

कार्यप्रणाली

- यह देखा गया है कि धोखेबाज एटीएम मशीन में स्किमिंग डिवाइस (डाटा चोरी करने की डिवाइस) इंसटॉल करते हैं और आपके कार्ड से डाटा चोरी करते हैं।
- नकली दिखावटी की-बोर्ड, साधारण नज़र से दिखाई न देने वाला अति लघु/पिनहोल कैमरा इंसटॉल करके पिन भी चुरा लिया जाता है।
- कभी - कभार, धोखेबाज अन्य ग्राहक का बहाना करके आपके पास में खड़े हो जाते हैं तथा जब आप पिन प्रविष्ट करते हैं, तो वे आपके पिन तक पहुँच प्राप्त कर लेते हैं।
- यह डेटा बाद में नकली कार्ड बनाने के लिए प्रयुक्त होता है एवं ग्राहक के खाते से राशि निकाल ली जाती है।

सावधानी

- यह सुनिश्चित करने के लिए लेनदेन करते समय इसकी जांच कर लें कि कार्ड प्रविष्ट करने के स्लॉट के पास या एटीएम मशीन के की - पैड में कोई अतिरिक्त उपकरण नहीं लगा हुआ है।
- अपना पिन डालते समय की-पैड को अपने हाथ से कवर करें/ढँक लें ।
- जब आपके नज़दीक कोई व्यक्ति खड़ा हो, तो उसकी उपस्थिति में अपना पिन नहीं डाले या किसी के साथ अपना कार्ड साझा नहीं करें।

6. स्क्रीन शेयरिंग एप/रिमोट एक्सेस के प्रयोग से धोखाधड़ी कार्यप्रणाली

- धोखेबाज आपको स्क्रीन शेयरिंग एप्स डाऊनलोड करने की युक्ति सुझाएंगे जिसके माध्यम से वे आपकी वित्तीय जानकारी तक पहुँचने हेतु आपके मोबाइल / लेपटॉप को नियंत्रित / देख सकते है।
- बाद में, वे आपके इन्टरनेट बैंकिंग / भुगतान एप का प्रयोग करके भुगतान करते हैं।

सावधानी

अनजान लोगों के साथ शेयर स्क्रीन को सक्रिय / एप डाऊनलोड नहीं करें।

7. सिम अदला - बदली / नकली सिम बनाना (सिम क्लोनिंग)

कार्यप्रणाली

- चूंकि अधिकांश खातों के ब्योरे और प्रमाणीकरण आपके पंजीकृत मोबाइल संख्या के साथ जुड़े होते हैं, धोखेबाज सिम कार्ड तक पहुंचने या नकली (डुप्लीकेट) सिम कार्ड प्राप्त करने की कोशिश करते हैं ताकि ऐसे नकली सिम कार्ड पर प्राप्त ओटीपी के प्रयोग से डिजिटल लेनदेन कर सकें।
- धोखेबाज सामान्यत: स्वयं को टेलीफोन / मोबाइल नेटवर्क का स्टाफ बताते हुए ग्राहक को फोन करते हैं तथा सिम कार्ड को 3जी से 4जी में नि:शुल्क अपग्रेड करने या सिम कार्ड पर अतिरिक्त लाभ देने के लिए ब्योरे प्रदान करने के लिए अनुरोध करते हैं।

सावधानी

- सिम कार्ड से संबंधित जानकारी कभी साझा नहीं करें।
- यदि सामान्य हालात में काफी समय तक आपके मोबाइल में नेटवर्क नहीं है, तो आपको तुरंत संदेहास्पद होना चाहिए और मोबाइल ऑपरेटर से यह सुनिश्चित करने के लिए संपर्क करें कि कहीं आपके सिम के लिए कोई नकली सिम जारी तो नहीं किया जा रहा है।

8. सर्च इंजन के माध्यम से प्राप्त असत्य सूचना के आधार पर निजी जानकारी (पासवर्ड इत्यादि) से छेड़छाड़ करके धोखाधड़ी

कार्यप्रणाली

- यह देखा गया है कि ग्राहक अपने बैंक, बीमा कंपनी, आधार अपडेशन केंद्र (सेंटर) इत्यादि का संपर्क ब्योरा/जानकारी प्राप्त करने हेतु सर्च इंजन का उपयोग करते हैं और सर्च इंजन पर दर्शाए गए अनजान / गैर सत्यापित संपर्क नंबर के साथ संपर्क कर बैठते हैं।
- धोखेबाजों द्वारा सर्च इंजन पर ये संपर्क जानकारियाँ अक्सर छद्म रूप में रहती है ताकि वे अपने शिकार को अपनी ओर आकर्षित कर सके।
- जब ग्राहक इनको कॉल करते हैं, तो ये बहुरूपिए ग्राहकों से सत्यापन के लिए उनके कार्ड के ब्योरे / जानकारी मांगते हैं।
- इस संपर्क / कॉल को सही / वास्तविक मानते हुए, लोग अपनी सभी सुरक्षित जानकारियों को साझा कर देते / हैं एवं इस प्रकार धोखे का शिकार हो जाते हैं।

सावधानी

सर्च इंजन पर कस्टमर केयर के संपर्क ब्योरे खोजने से बचें। ये ब्योरें अक्सर धोखेबाजों के द्वारा छद्म रूप में रहते हैं। किसी को भी हमेशा संपर्क ब्योरा/जानकारी प्राप्त करने के लिए बैंक / कंपनियों की आधिकारिक वेबसाइट का उपयोग करना चाहिए।

9. क्यूआर कोड स्केन के द्वारा घोटाला

कार्यप्रणाली

धोखेबाज अक्सर विभिन्न प्रकार के बहानों के साथ ग्राहकों से संपर्क करते हैं एवं उनको भुगतान एप्स के माध्यम से क्यूआर कोड स्केन के लिए फँसाते हैं। इससे धोखेबाज व्यक्ति ग्राहकों के खाते से धन निकाल लेते है।

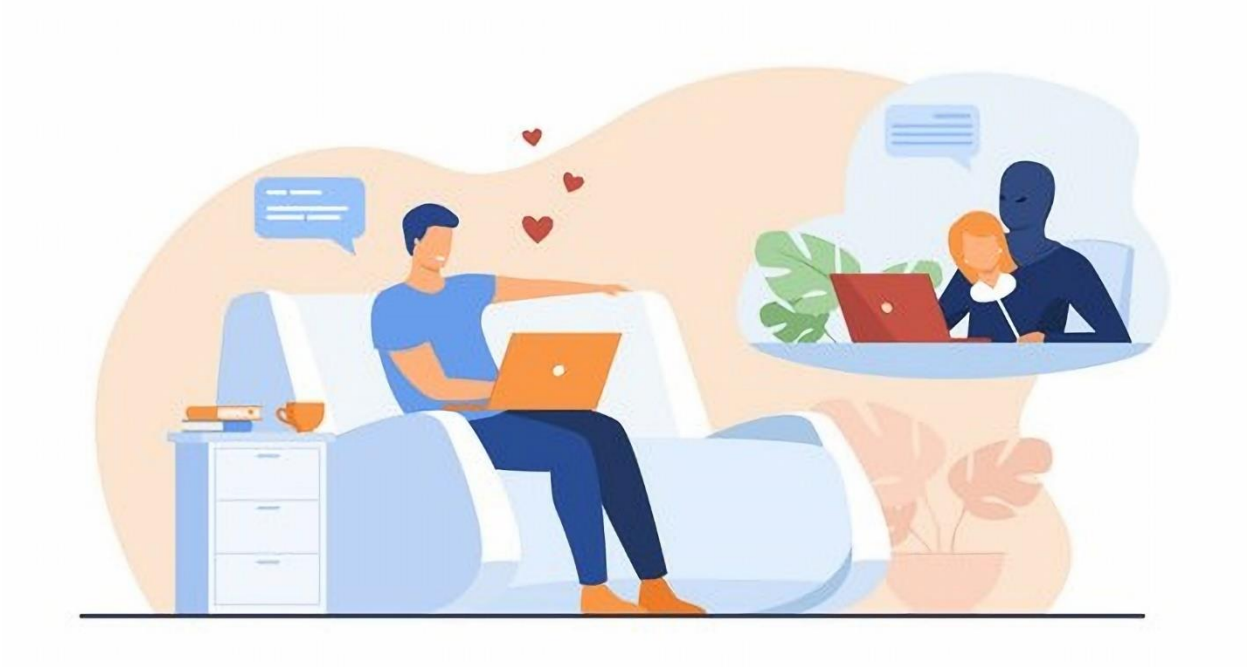
सावधानी

भुगतान एप्स का उपयोग करके कोई भी क्यूआर कोड स्केन करते समय सावधानरहें। क्यूआर कोड में खाते का ब्योरा रहता जिससे किसी विशिष्ट खाते में राशि अंतरित की जाती है।

10. सोशल मीडिया के माध्यम से नकली पहचान धारण करना

कार्यप्रणाली

- धोखेबाज व्यक्ति लोकप्रिय/प्रसिद्ध सोशल मीडिया प्लेटफ़ोर्म्स जैसे फेसबुक व इंस्टाग्राम पर नकली / जाली अकाउंट बनाते हैं। उसके बाद वे आपके मित्रों को अत्यावश्यक चिकित्सा (मेडिकल) उद्देश्यों, भुगतानों इत्यादि के लिए धन हेतु अनुरोध भेजते हैं।
- धोखेबाज कुछ समय के बाद विश्वास भी हासिल कर लेते हैं और बाद में निजी जानकारी का उपयोग ब्लेकमेल व जबर्दस्ती धन वसूली के लिए करते हैं।



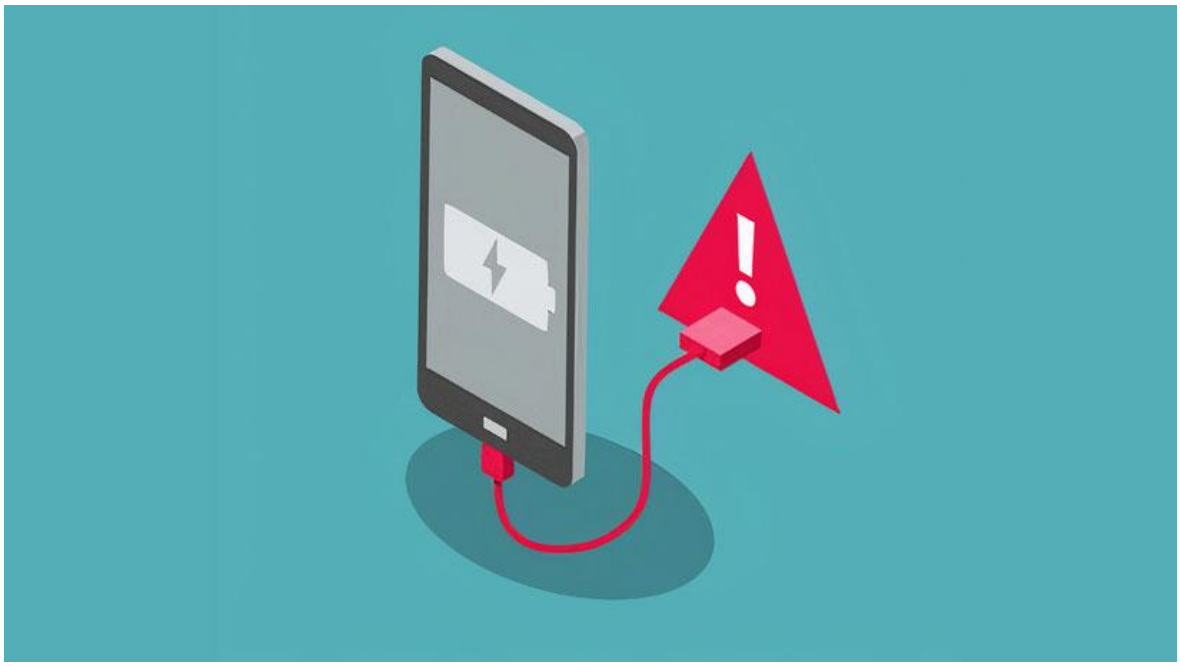
सावधानी

- अनजान व्यक्तियों को ऑनलाइन भुगतान न करें।
- सोशल मीडिया प्लेटफोर्म्स पर निजी एवं गोपनीय जानकारी साझा न करें।
- निधियों/धन आदि के अनुरोध की सच्चाई/वास्तविकता को जांचने के लिए हमेशा मित्र / संबंधी से फोन कॉल या प्रत्यक्ष रूप से मिलकर इस बात की पुष्टि कर ली जाए कि प्रोफाइल नकली तो नहीं है।

11. ज्यूस जैकिंग (चार्जिंग पोर्ट के माध्यम से साइबर क्राइम)

कार्यप्रणाली

- मोबाइल का चार्जिंग पोर्ट का उपयोग फाइल / डाटा ट्रांसफर करने के लिए भी किया जा सकता है।
- ज्यूस जैकिंग, एक प्रकार की साइबर चोरी है, जहां पर आपका मोबाइल अनजान / गैर सत्यापित चार्जिंग पॉर्ट्स से जोड़ा जाता है तो अनजान एप्स / मैलवेयर अपने आप इंस्टॉल हो जाता है जिससे धोखेबाज संवेदनशील डेटा / ईमेल / एसएमएस, सहजे गए पासवर्ड्स तक पहुँच / नियंत्रित कर / चुरा सकते हैं।



सावधानी

हमेशा पब्लिक / अनजान चारजिंग पॉर्ट्स / कैबल्स का उपयोग करने से बचें।

12. लॉटरी धोखाधड़ी

कार्यप्रणाली

- धोखेबाज आपको ईमेल भेजेंगे / फोन करेंगे कि आपने अभी-अभी एक बहुत बड़ी लॉटरी जीती है और वे कहेंगे कि धन प्राप्त करने के लिए आपके पहचान की पुष्टि किए जाने के लिए यह अपेक्षित है कि उनकी वेबसाइट्स पर आपके बैंक खाते/ क्रेडिट कार्ड के माध्यम से आपकी जांच की जाए। ऐसा करके वे आपका डेटा ले लेते हैं।
- कुछ मामलों में, धोखेबाज द्वारा लॉटरी / उत्पाद प्राप्त करने हेतु पहले टैक्स, शिपिंग चार्जेज, प्रोसेसिंग फीस इत्यादि के भुगतान के लिए कहते हैं।
- चूंकि, लॉटरी / इनाम की अनुरोध की गई राशि बहुत ही कम प्रतिशत की होती है, शिकार धोखेबाज के जाल में फंस जाते हैं और भुगतान कर देते हैं।

सावधानी

लॉटरी के लिए आने वाले कॉल्स / ईमेल के लिए भुगतान नहीं करें या सुरक्षित जानकारी साझा नहीं करें। जब भी आपके पास कोई ऐसी अविश्वसनीय लॉटरी / प्रस्ताव आए, तो हमेशा शंका करें।

13. ऑनलाइन जॉब धोखाधड़ी

कार्यप्रणाली

- नौकरी ढूंढने के जाली पोर्टल बनाए जाते हैं और जब शिकार व्यक्ति / इन वेबसाइट्स पर पंजीकरण के लिए बैंक खाते / डेबिट कार्ड / क्रेडिट कार्ड की सुरक्षित जानकारी साझा करते हैं, आपके खाते से छेड़छाड़ हो जाती है।
- कुछ मामलों में, धोखेबाज स्वयं को प्रतिष्ठित कंपनी के अधिकारी बताते हैं और नकली/जाली साक्षात्कार करने के पश्चात चयन की पुष्टि करते हैं। शिकार को अनिवार्य प्रशिक्षण कार्यक्रम इत्यादि के भुगतान हेतु उकसाया जाता है।

सावधानी

- हमेशा याद रखें कि एक वास्तविक कंपनी, जो नौकरी दे रही है, वह कभी भी धन की मांग नहीं करेगी।
- अनजान जॉब पोर्टल पर भुगतान नहीं करें।

.

गैर बैंकिंग वित्तीय कंपनियों में कपटपूर्ण लेनदेन की कार्य प्रणाली और बरती जाने वाली सावधानियाँ

1. धोखेबाजों द्वारा ऋण प्रदान करने के लिए नकली / जाली विज्ञापन

- धोखेबाज अत्यंत आकर्षक कम ब्याज दरों या आसान पुनर्भुगतान तरीकों या बिना किसी प्रतिभूति की आवश्यकता इत्यादि पर पर्सनल लोन देने वाली नकली/जाली विज्ञापन जारी करते हैं एवं ग्राहकों को उनसे संपर्क करने के लिए कहते हैं।
- भोले-भाले ग्राहकों की विश्वसनीयता हासिल करने तथा विश्वास पैदा करने/जगाने के लिए, ये ई मेल आईडी, गैर बैंकिंग वित्तीय कंपनियों के मशहूर/सुपरिचित / वास्तविक वरिष्ठ अधिकारियों के ईमेल आईडी के तरह लगते हैं।
- जब ग्राहक लोन लेने के लिए धोखेबाज से संपर्क करते हैं तो धोखेबाज विभिन्न प्रकार के पूर्व शुल्क यथा प्रोसेसिंग फीस, जीएसटी, अन्तर नगर प्रशुल्क, अग्रिम ईएमआई, अनहोल्ड चार्जेज इत्यादि लेते हैं और ऋण संवितरित किए बिना फरार हो जाते हैं।
- धोखेबाज सर्च इंजन पर दिखाने के लिए नकली/जाली वेबसाइट्स लिंक भी बनाते हैं, जिससे लोग लोन इत्यादि तलाशने के लिए सर्च करते हैं।

सावधानी

- गैर बैंकिंग वित्तीय कंपनियाँ / बैंक ऋण आवेदन की प्रोसेसिंग के पहले कभी भी अग्रिम शुल्क की मांग नहीं करते।
- बैंक / गैर बैंकिंग वित्तीय कंपनियाँ प्रोसेसिंग शुल्क लेती हैं, जो कि ऋण राशि में से काटा जाता है।
- कम ब्याज दरों इत्यादि पर ऑनलाइन ऋण प्रस्ताव पर वास्तविक स्त्रोत से विवरण जाँचे बगैर भुगतान नहीं करें या अपनी सुरक्षित जानकारी को प्रविष्ट नहीं करें।

2. एसएमएस / ईमेल / इंस्टेंट मैसेजिंग / कॉल स्कैम

- धोखेबाज आकर्षक ऋणों की उपलब्धता के बारे में इंस्टेंट मैसेंजर/एसएमएस/सोशल मीडिया के माध्यम से फर्जी संदेश परिचालित करते हैं और विश्वसनीयता पैदा करने के लिए उनके द्वारा साझा किए गए मोबाइल नंबर से किसी भी ज्ञात एनबीएफसी के लोगो चित्र (logo) को प्रोफ़ाइल चित्र के रूप में उपयोग करते हैं। धोखेबाज अपना आधार कार्ड/पैन कार्ड और नकली एनबीएफसी पहचान पत्र (आईडी कार्ड) भी साझा करते हैं।

- ऋण लेने/चाहने वालों को ऐसे बल्क संदेश/एसएमएस/ईमेल भेजने के बाद, धोखेबाज यादृच्छिक लोगों को बुलाते हैं और नकली मंजूरी पत्र, नकली चेक की प्रतियां, आदि साझा करते हैं, और विभिन्न शुल्कों की मांग करते हैं। यदि एक बार शिकार ने इन शुल्कों का भुगतान कर दिया, तो जालसाज पैसे लेकर फरार हो जाते हैं और शिकार/ को उसके पैसे वापस पाने की बहुत कम संभावना के साथ छोड़ देता है।

सावधानियाँ

- एसएमएस/ईमेल के माध्यम से भेजे गए लिंक पर कभी भी क्लिक न करें या विज्ञापन संबंधी ऐसे एसएमएस/ईमेल का जवाब न दें।
- संदिग्ध अटैचमेंट या फ़िशिंग लिंक भेजने वाले अज्ञात स्रोतों के ईमेल को कभी भी न खोलें/उनका जवाब न दें।
- कभी भी लोगों द्वारा टेलीफोन/ईमेल आदि के माध्यम से दिए गए ऋण प्रस्तावों पर विश्वास न करें।
- इस तरह के प्रस्तावों के लिए कभी भी कोई भुगतान न करें अथवा ऐसे प्रस्तावों के लिए किसी भी व्यक्तिगत / वित्तीय जानकारी को अन्य स्रोतों के माध्यम से उसके वास्तविक होने के के बारे में क्रॉस-चेक किए बिना साझा न करें।

3. ओटीपी आधारित धोखाधड़ी

- शिकार को एनबीएफसी के रूप में लगने वाले धोखेबाजों से एसएमएस / त्वरित संदेश प्राप्त होते हैं जो ऋण अथवा क्रेडिट सीमा में वृद्धि की पेशकश करते हैं और कहा जाता है कि धोखेबाजों के मोबाइल नंबर पर संपर्क करें।

- जब शिकार /पीड़ित व्यक्ति उस नंबर पर कॉल करते हैं तो धोखेबाज उनसे वित्तीय विवरण वाले कुछ फॉर्म (यहां तक कि ऑनलाइन) भरने के लिए कहते हैं और वे उन्हें ओटीपी या पिन विवरण साझा करने के लिए भी उकसाते / मनाते हैं, जिसके परिणामस्वरूप उनको पैसे/आर्थिक हानि होती है।

सावधानियां

- अपना ओटीपी/पिन नंबर/व्यक्तिगत विवरण आदि से संबन्धित जानकारी किसी भी रूप में किसी के साथ साझा न करें।
- आपकी जानकारी के बिना कोई ओटीपी जनरेट नहीं हुआ है, यह सुनिश्चित करने के लिए नियमित रूप से अपने एसएमएस / ईमेल की जांच करें।

4. नकली (फर्जी) ऋण वेबसाइट / ऐप धोखाधड़ी (फ्रॉड)

- ऐसे कई बेईमान/अनैतिक ऋण ऐप हैं जो तत्काल और अल्पकालिक ऋण प्रदान करते हैं। ये ऐप उधारकर्ताओं को ठगते हैं और काफी अधिक दर पर ब्याज भी वसूलते हैं।

- भोले-भाले ग्राहकों को आकर्षित करने के लिए, ये धोखेबाज "सीमित अवधि ऑफ़र" का विज्ञापन करते हैं और आवेदकों को स्केयरवेयर युक्ति/चालों का उपयोग करके तत्काल निर्णय लेने के लिए उकसातेहैं।

सावधानियां

संदिग्ध ऋण ऐप आदि से ऋण लेने से पहले निम्नलिखित बातों का ध्यान रखें।

- क्या ऋणदाता क्रेडिट स्कोर की जांच करने के बजाय व्यक्तिगत विवरण जानने में अधिक रुचि रखता है?
- क्या ऋणदाता सरकार / अधिकृत एजेंसियों के साथ पंजीकृत है?
- जाँच करें कि क्या ऋणदाता ने कोई भौतिक (प्रत्यक्ष) पता या संपर्क जानकारी दी है; अन्यथा अंतिम क्षण उनसे संपर्क करना मुश्किल हो सकता है।
- याद रखें कि कोई भी प्रतिष्ठित एनबीएफसी / बैंक ऋण आवेदन को संसाधित करने से पहले कभी भी भुगतान के लिए नहीं कहेगा।
- वास्तविक ऋण प्रदाता कभी भी दस्तावेजों को सत्यापित किए बिना राशि/ पैसे नहीं देते हैं।
- यह जांच करें कि क्या ये एनबीएफसी-समर्थित ऋण ऐप्स वास्तविक हैं।

5. मनी सर्कुलेशन/पोंजी/मल्टी लेवल मार्केटिंग (एमएलएम) योजनाएं धोखाधड़ी

- एमएलएम/श्रृंखला विपणन (Chain Marketing) /पिरामिड संरचना योजनाएं नामांकन/ सदस्यों को जोड़ने पर आसान या त्वरित राशि/धन का वादा करती हैं।

- ऐसी योजनाओं द्वारा न केवल उच्च रिटर्न का आश्वासन दिया जाता है बल्कि भोले-भाले लोगों का विश्वास हासिल करने के लिए अपने वादे के अनुसार पहली कुछ किश्तों का भुगतान भी करते हैं और मौखिक प्रचार के माध्यम से अधिक निवेशकों को आकर्षित करते हैं।

- ऐसी योजनाएँ अधिक से अधिक लोगों को श्रृंखला / समूह में शामिल होने के लिए प्रोत्साहित करती हैं, जिसके लिए उत्पादों की बिक्री से कमीशन के बजाय नामांकनकर्ता को कमीशन का भुगतान किया जाता है।

- इस मॉडल के कारण, कुछ समय बाद जब योजना में शामिल होने वाले लोगों की संख्या कम होने लगती है तो यह योजना अस्थिर हो जाती है। इसके बाद, धोखेबाज़ योजना को बंद कर देते हैं और लोगों द्वारा निवेश किए गए धन को लेकर गायब हो जाते हैं।

सावधानियां: पोंजी/एमएलएम योजनाओं में निवेश करते समय

- प्रतिफल जोखिम के समानुपाती होते हैं। जितना अधिक रिटर्न, उतना अधिक जोखिम। इसलिए, यदि कोई योजना लगातार असामान्य रूप से उच्च रिटर्न दे रही है, (जैसे कि हर साल 40-50 प्रतिशत) यह संभावित धोखाधड़ी और सावधानी बरतने का पहला संकेत है।

- हमेशा ध्यान दें कि वस्तु//सेवा की वास्तविक बिक्री के बिना होने वाला कोई भुगतान/ कमीशन/ बोनस/ लाभ का प्रतिशत संदेहास्पद है और इससे धोखाधड़ी हो सकती है।

- मल्टी-लेवल मार्केटिंग / चेन मार्केटिंग / पिरामिड स्ट्रक्चर स्कीम चलाने वाली संस्थाओं द्वारा दिए गए उच्च रिटर्न के वादों से जनता को लुभावन नहीं होना चाहिए।

- प्राइज चिट एंड मनी सर्कुलेशन (प्रतिबंध) अधिनियम 1978 के तहत मनी सर्कुलेशन / मल्टी-लेवल मार्केटिंग / पिरामिड संरचनाओं के तहत राशि/धन स्वीकारना या लेना एक संज्ञेय (हस्तक्षेप योग्य) अपराध है।ऐसे प्रस्तावों से सामना होने पर जनता द्वारा राज्य पुलिस के पास तुरंत शिकायत दर्ज की जानी चाहिए।

6. जाली दस्तावेज़ों के साथ धोखाधड़ी युक्त ऋण

- जाली दस्तावेज़ के साथ धोखाधड़ी एक ऐसी धोखाधड़ी है जिसमें कोई व्यक्ति या संस्था वित्तीय संस्थानों से किसी भी प्रकार की सेवाओं का लाभ उठाने के लिए जाली दस्तावेज़ों का उपयोग करती है।

- ऐसी धोखाधड़ी एनबीएफसी कर्मचारी की प्रामाणिकता / एनबीएफसी की ईमेल आईडी की प्रामाणिकता की जांच किए बिना संस्थाओं के साथ केवाईसी से संबंधित दस्तावेजों को साझा करते समय होती है।

- पीड़ित की व्यक्तिगत जानकारी जैसे पहचान पत्र, बैंक खाता विवरण, आदि चुराकर नकली दस्तावेजों के आधार पर भी फर्जी ऋण स्वीकृत किए जाते हैं और किसी वित्तीय संस्थान से लाभ प्राप्त करने के लिए इस जानकारी या क्रेडेंशियल का उपयोग किया जाता है।

सावधानियाँ

- किसी भी संस्था से ऋण लेते समय ग्राहकों को केवाईसी और ऋण के वितरण के बाद एनएसीएच फॉर्म सहित अन्य व्यक्तिगत दस्तावेज देते समय सतर्क रहना चाहिए।

- ऐसे दस्तावेज़ केवल संस्था के अधिकृत कर्मियों या अधिकृत ईमेल आईडी के साथ साझा किए जाने चाहिए।

- साथ ही, ऋण की स्वीकृति न होने और ऋण के बंद होने के बाद, ग्राहक को हमेशा संस्थाओं से अनुरोध करना चाहिए के वे ग्राहकों द्वारा संस्थाओं को दिए गए दस्तावेजों को वापस करें।

वित्तीय लेनदेन करते समय बरती जाने वाली अन्य सामान्य सावधानियां

सामान्य

- आपके ब्राउज़िंग सत्र के दौरान संदिग्ध रूप से दिखाई देने वाले पॉप अप से सावधान रहें।
- ऑनलाइन भुगतान करने से पहले हमेशा एक सुरक्षित भुगतान गेटवे की जांच करें (https:// - पैड लॉक सिंबल वाला यूआरएल) ।
- अपना पिन (व्यक्तिगत पहचान संख्या), पासवर्ड, और क्रेडिट अथवा डेबिट कार्ड नंबर, सीवीवी निजी रखें।
- वेबसाइटों/उपकरणों/सार्वजनिक लैपटॉप/डेस्कटॉप पर कार्ड विवरण सहेजने (सेव करने) से बचें।
- जहां सुविधा उपलब्ध हो वहां टू-फैक्टर ऑथेंटिकेशन ऑन करें।
- संदिग्ध अटैचमेंट या फ़िशिंग लिंक वाले अज्ञात स्रोतों के ईमेल कभी भी न खोलें।
- चेकबुक, केवाईसी दस्तावेजों की प्रतियां कभी भी अजनबियों के साथ साझा न करें।

उपकरण (डिवाइस) / कंप्यूटर की सुरक्षा के लिए

- नियमित अंतराल पर पासवर्ड बदलें।
- डिवाइस पर एंटीवायरस इंस्टॉल करें और जब भी उपलब्ध हो अपडेट इंस्टॉल करें।
- उपयोग करने से पहले हमेशा अज्ञात यूएसबी ड्राइव/डिवाइस को स्कैन करें।
- अपने डिवाइस को खुला न छोड़ें।
- निर्दिष्ट समय के बाद डिवाइस के ऑटो लॉक को कॉन्फ़िगर करें।
- अज्ञात एप्लिकेशन या सॉफ़्टवेयर इंस्टॉल न करें।
- अज्ञात उपकरणों पर पासवर्ड या गोपनीय जानकारी संग्रहीत (सेव) न करें।

सुरक्षित इंटरनेट ब्राउज़िंग के लिए

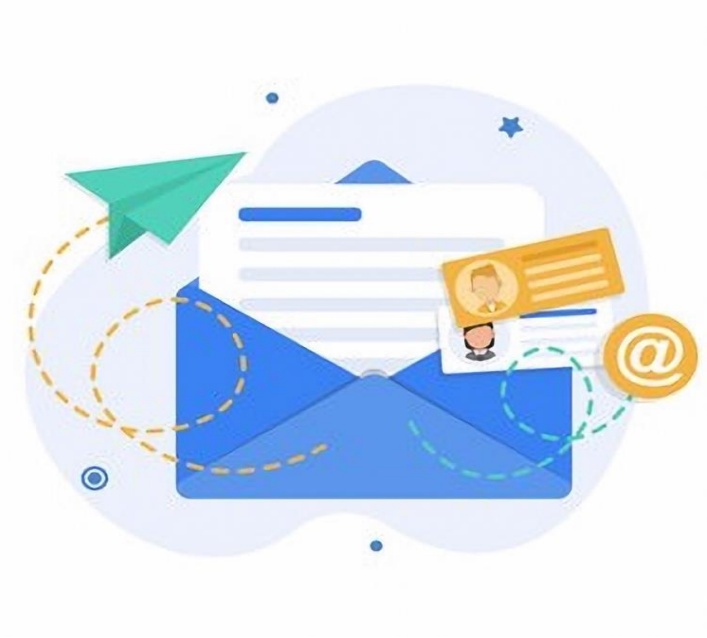
- असुरक्षित वेबसाइटों पर जाने से बचें।
- अनजान ब्राउजर के इस्तेमाल से बचें।
- सार्वजनिक उपकरणों पर पासवर्ड सहेजने (सेव करने) से बचें।
- अज्ञात वेबसाइटों पर सुरक्षित जानकारी (क्रेडेंशियल) डालने से बचें।
- सोशल मीडिया पर अनजान व्यक्तियों से निजी जानकारी साझा न करें।
- ईमेल अथवा एसएमएस लिंक पुनर्निर्देशित होने की स्थिति में, पृष्ठ की सुरक्षा को हमेशा जांच लें / सत्यापित करें।

सुरक्षित इंटरनेट बैंकिंग के लिए

- सार्वजनिक उपकरणों पर हमेशा वर्चुअल कीबोर्ड का उपयोग करें क्योंकि कीस्ट्रोक्स को कॉमप्रोमाइज़ किए गए उपकरणों, कीबोर्ड आदि के माध्यम से भी कैप्चर किया जा सकता है।
- उपयोग के तुरंत बाद इंटरनेट बैंकिंग सत्र से लॉग आउट करें।
- समय-समय / आवधिक आधार पर पासवर्ड अपडेट करते रहें।
- ईमेल और इंटरनेट बैंकिंग के लिए एक जैसे पासवर्ड का इस्तेमाल न करें।
- वित्तीय लेनदेन के लिए सार्वजनिक टर्मिनलों (जैसे साइबर कैफे, आदि) का उपयोग करने से बचें।

ई-मेल अकाउंट सुरक्षा के लिए

- अनजान पतों (एड्रेस) से प्राप्त ईमेल पर क्लिक न करें।
- सार्वजनिक या मुफ्त नेटवर्क पर ईमेल का उपयोग करने से बचें।
- ईमेल में सुरक्षित जानकारी (क्रेडेंशियल) / बैंक पासवर्ड आदि को स्टोर न करें।



पासवर्ड सुरक्षा के लिए

- अपने पासवर्ड में अक्षरांकीय (अल्फान्यूमेरिक) और विशेष वर्णों (स्पेशल करेक्टर) के संयोजन का उपयोग करें।
- सुविधा उपलब्ध होने पर अपने सभी खातों के लिए टू फैक्टर ऑथेंटिकेशन रखें ।
- समय-समय / आवधिक आधार पर पासवर्ड बदलें।

आपको कैसे पता चलेगा जमा कि जमाराशियाँ करने वाली एनबीएफसी असली है या नहीं?

- जमाकर्ता को यह जांच करना चाहिए कि क्या जमाराशियां स्वीकार करने के लिए पात्र एनबीएफसी जमाराशियां लेनेवाली एनबीएफसी की सूची में मौजूदहैं, जो https://rbi.org.in पर उपलब्ध है और सुनिश्चित करें कि एनबीएफ़सी का नाम जमाराशियां स्वीकार करने से प्रतिबंधित कंपनियों की सूची में तो नहीं दिख रहा है।
- एनबीएफसी को अपनी साइट पर रिज़र्व बैंक द्वारा जारी पंजीकरण प्रमाणपत्र (सीओआर) को प्रमुखता से प्रदर्शित करना आवश्यक है। यह प्रमाणपत्र यह भी दर्शाता कि एनबीएफसी को विशेष रूप से आरबीआई द्वारा जमाराशियां स्वीकार करने के लिए अधिकृत किया गया है। उक्त को सुनिश्चित करने के लिए जमाकर्ताओं को प्रमाणपत्र की जांच करनी चाहिए कि एनबीएफसी जमाराशियां स्वीकार करने के लिए अधिकृत है अथवा नहीं।
- एनबीएफसी 12 महीने से कम और 60 महीने से अधिक की अवधि के लिए जमाराशियां स्वीकार नहीं कर सकती हैं और एनबीएफसी द्वारा जमाकर्ता को दी जाने वाली अधिकतम ब्याज दर 12.5% से अधिक नहीं होनी चाहिए।
- रिजर्व बैंक द्वारा ब्याज दरों में बदलाव को https://rbi.org.in → साइटमैप → एनबीएफसी सूची → अक्सर पूछे जाने वाले प्रश्न पर प्रकाशित किया जाता है।

जमाकर्ताओं द्वारा बरती जाने वाली सावधानियां

- जमाकर्ता द्वारा कंपनी के पास जमा की गई प्रत्येक जमा राशि के लिए एक उचित रसीद प्रदान करने पर जोर देना चाहिए।
- रसीद पर कंपनी द्वारा अधिकृत अधिकारी द्वारा विधिवत हस्ताक्षर किया जाना चाहिए और रसीद पर जमा करने की तारीख, जमाकर्ता का नाम, शब्दों और अंकों में राशि, देय ब्याज दर, परिपक्वता तिथि और राशि का उल्लेख होना चाहिए।
- गैर-बैंकिंग वित्तीय कंपनियों की ओर से जनता की जमाराशियां एकत्रित करने वाले दलालों / एजेंटों आदि के मामले में, जमाकर्ताओं को इस बात से स्वयं को संतुष्ट होना चाहिए कि दलाल / एजेंट एनबीएफसी द्वारा विधिवत रूप से अधिकृत किया गया है।
- जमाकर्ता को यह ध्यान रखना चाहिए कि एनबीएफसी के जमाकर्ताओं के लिए जमा बीमा सुविधा उपलब्ध नहीं है।

ऑनलाइन शिकायत कैसे करें

आरबीआई से शिकायत

➢ कृपया https://cms.rbi.org.in लिंक पर जाएं

सेबी को शिकायत

➢ कृपया https://scores.gov.in पर दिए गए लिंक पर जाएं

भारतीय बीमा नियामक और विकास प्राधिकरण (IRDAI) को शिकायत

➢ कृपया https://igms.irda.gov.in/ पर दिए गए लिंक पर जाएं

राष्ट्रीय आवास बैंक (एनएचबी) को शिकायत

➢ कृपया https://grids.nhbonline.org.in पर लिंक पर जाएं।

साइबर पुलिस स्टेशन में शिकायत

➢ कृपया https://cybercrime.gov.in देखें

शब्दावली*

- **अग्रिम शुल्क/प्रसंस्करण शुल्क/टोकन शुल्क:** इसका अर्थ है ऐसे सभी प्रारंभिक भुगतान जो दस्तावेज़ प्रतिपूर्ति तक सीमित नहीं होंगे, खर्च पूरा करने वाले होंगे, जिनपर लागू प्रसंस्करण शुल्क और कोई अन्य लागू शुल्क जो उधारकर्ता को ऋण के वितरण के लिए लगाया जा सकता है।
- **दो तरीकों से प्रमाणीकरण:** दो-कारक प्रमाणीकरण (जिसे 2FA के रूप में भी जाना जाता है) उपयोगकर्ताओं को दो अलग-अलग घटकों के संयोजन के माध्यम से स्पष्ट पहचान प्रदान करता है, एक जो आपके पास है - कार्ड (नंबर, समाप्ति तिथि और सीवीवी जो कार्ड पर छपा हुआ है), जिसे आप जानते हैं - मान्य करने के लिए पिन (या तो स्थायी / स्थिर अथवा एक बार के लिए उत्पन्न)।
- **3-डी सुरक्षित:** 3-डी सिक्योर एक एक्सएमएल-आधारित प्रोटोकॉल है जिसे ऑनलाइन क्रेडिट और डेबिट कार्ड लेनदेन के लिए एक अतिरिक्त सुरक्षा परत (लेयर) के रूप में डिजाइन किया गया है। इसे वेरिफाइड बाय वीज़ा, मास्टरकार्ड सिक्योर कोड या अमेरिकन एक्सप्रेस सेफ-की के नाम से भी जाना जाता है।
- **अधिग्रहण बैंक:** अधिग्रहण बैंक वह बैंक है जो क्रेडिट या डेबिट कार्ड को प्रोसेस करता है। अधिग्रहण करने वाला बैंक आमतौर पर कई कार्ड योजनाओं जैसे वीज़ा, मास्टरकार्ड, मेस्ट्रो और रुपे को सपोर्ट करता है।
- **प्राधिकरण:** कार्ड जारी करने वाले बैंक की ओर से व्यापारी द्वारा प्राप्त लेन-देन प्राधिकरण अनुरोध पर प्रतिक्रिया यह दर्शाती है कि भुगतान जानकारी मान्य है और ग्राहक के क्रेडिट कार्ड पर फंड उपलब्ध हैं।
- **बैंक पहचान संख्या (बीआईएन):** अपने प्रत्येक सदस्य वित्तीय संस्थानों, बैंकों और प्रोसेसरों को वीज़ा और मास्टरकार्ड द्वारा आवंटित / निर्दिष्ट एक पहचान संख्या।
- **बिन (BIN) वैधता / सत्यापन:** प्रतिभागी बिन सूची के विरुद्ध कार्ड के बिन की जाँच करने की प्रक्रिया।
- **ब्लेकलिस्ट (प्रतिबंधित सूची) में डालना:** धोखाधड़ी को रोकने के उद्देश्य से धोखेबाज खरीदारों या उच्च जोखिम वाले व्यापारियों का पता लगाने के लिए जानकारी एकत्र करने की प्रथा।

(*स्रोत-इंटरनेट और अन्य प्रकाशन)

- **कार्ड कैप्चर पेज**
  सुरक्षित पृष्ठ जिस पर कार्ड के विवरण कैप्चर किए गए हैं। जिन संस्थाओं के पास PCI DSS प्रमाणन है, उन्हें कार्ड विवरण प्राप्त करने की अनुमति है। उन संस्थानों के उदाहरण जिनके पास कार्ड कैप्चर पृष्ठ है।
  - अधिग्रहण बैंक (जैसे एसबीआई, एचडीएफसी)
  - एग्रीगेटर (जैसे, पेयू PayU)
  - मर्चेंट (जैसे, फ्लिपकार्ट, अमेज़न)
- **कार्ड नंबर**
  - क्रेडिट कार्ड एसोसिएशन या कार्ड जारी करने वाले बैंक द्वारा कार्डधारक को दी गई / आवंटित की गई खाता संख्या। क्रेडिट कार्ड से भुगतान करने के लिए किसी ग्राहक द्वारा किसी व्यापारी को यह जानकारी प्रदान की जानी चाहिए।
  - कार्ड के ऊपर छपे अंकों की स्ट्रिंग (ये अंक बैंड पहचान संख्या, श्रेणी, करेंसी आदि को दर्शाते हैं)
  - वीज़ा, मास्टरकार्ड, मेस्ट्रो, रुपे: 16 अंक
  - एमेक्स: 15 अंक
- **कार्ड प्रेजेंट (सीपी):** लेन-देन के दौरान, कार्डधारक अथवा कार्ड बिक्री के स्थान पर कार्ड को प्रस्तुत किया जाता है। उदाहरण: किराने की दुकान पर कार्ड स्वाइप किया गया। आमतौर पर सीपी मामलों में टीडीआर/एमडीआर कार्ड नॉट प्रेजेंट (सीएनपी) मामलों से कम होते हैं क्योंकि सीपी लेनदेन में जोखिम कम होता है (दरें जोखिम के लिए समायोजित की जाती हैं)।
- **कार्ड वॉल्टिंग:** कार्ड विवरण (कार्ड नंबर और सीवीवी) संग्रहीत करने की प्रक्रिया और बाद के लेनदेन के दौरान संग्रहीत कार्ड विवरण दिखाएं। कार्ड को पीसीआई डीएसएस प्रमाणित संस्था (बैंक, एग्रीगेटर या मर्चेंट का अधिग्रहण) द्वारा स्टोर किया जा सकता है।
- **क्लोज्ड-लूप प्रीपेड कार्ड/वॉलेट:** कार्ड/वॉलेट जिनका उपयोग केवल एक ही व्यापारी द्वारा किया जा सकता है और धन को स्रोत खाते में या एटीएम के माध्यम से नहीं निकाला जा सकता है।
- **को-ब्रांडेड कार्ड:** ऐसे कार्ड जो एक वित्तीय संस्थान द्वारा किसी कार्ड योजना के साथ जारी किए जाते हैं और जिनमें कॉर्पोरेट ब्रांडिंग होती है।
- **संग्रह खाता:** व्यापारी का बैंक खाता जिसमें भुगतान गेटवे की आय जमा की जाती है। संग्रह खाता कोई चालू खाता, नोडल खाता या एस्क्रो खाता हो सकता है।

- **क्रेडिट कार्ड:** वे कार्ड जो किसी वित्तीय संस्थान से पैसे उधार लेकर उत्पादों या सेवाओं के लिए भुगतान करने की अनुमति देते हैं।
- **शुल्क-वापसी**
  - o क्रेडिट कार्डधारक द्वारा जारीकर्ता बैंक के साथ उठाया गया विवाद।
  - o शुल्क वापसी के कई कारण हो सकते हैं:
  - • सेवा/उत्पाद डिलीवर नहीं किया गया
  - • रद्द करने पर धन वापसी जारी नहीं की गई है
  - • संदिग्ध धोखाधड़ी लेनदेन
  - • कार्ड हैक किया जा रहा है
- ऐसी परिस्थितियों में, जारीकर्ता बैंक अधिग्रहणकर्ता बैंक को चार्जबैक भेजेगा और अधिग्रहण करने वाला बैंक सीधे व्यापारी तक पहुंचता है (यदि अधिग्रहण करने वाले बैंक का व्यापारी के साथ सीधा एकीकरण है) या एग्रीगेटर (यदि लेनदेन एग्रीगेटर के माध्यम से संसाधित किया जाता है) के माध्यम से निर्धारित समय के भीतर वितरण या धनवापसी का समर्थन करने के लिए सबूत प्रदान करने के लिए अन्यथा चार्जबैक मान्य माना जाएगा और व्यापारी चार्जबैक राशि वापस करने के लिए बाध्य होगा।
- **क्रेडिट लिमिट:** क्रेडिट लिमिट से तात्पर्य उस अधिकतम राशि से है जो कोई वित्तीय संस्थान किसी ग्राहक को देता है। एक उधार देने वाला संस्थान क्रेडिट कार्ड या क्रेडिट की एक लाइन पर क्रेडिट सीमा बढ़ाता है। ऋणदाता आमतौर पर क्रेडिट चाहने वाले आवेदक द्वारा दी गई जानकारी के आधार पर क्रेडिट सीमा निर्धारित करते हैं। क्रेडिट सीमा एक ऐसा कारक है जो उपभोक्ताओं के क्रेडिट स्कोर को प्रभावित करता है और भविष्य में क्रेडिट प्राप्त करने की उनकी क्षमता को प्रभावित कर सकता है।
- **सीवीवी** - कार्ड सत्यापन मूल्य मान को दर्शाता है। यह संख्या ऑनलाइन लेनदेन को पूरा करने के लिए महत्वपूर्ण है और इसे कभी भी किसी के साथ साझा नहीं किया जाना चाहिए।
- **डेबिट कार्ड:** वे कार्ड जो खरीदारी करने के लिए बैंक खाते में उपलब्ध धनराशि की स्वत: कटौती के माध्यम से काम करते हैं।
- **अस्वीकृत भुगतान:** कार्ड जारी करने वाले बैंक द्वारा लेन-देन को स्वीकृत नहीं किए गए और उसे अस्वीकृत के रूप में चिह्नित किया जाता है। अस्वीकृत लेनदेन के लिए आगे कोई कार्रवाई नहीं की जा सकती है और ग्राहक को भुगतान करने के लिए पुनः प्रयास करना होगा।

- **डिजिटल हस्ताक्षर:** एक ऐसी इलेक्ट्रॉनिक फ़ाइल जिसमें अद्वितीय जानकारी होती है जिसका उपयोग किसी संगठन या व्यक्ति की विश्वसनीयता को सत्यापित करने के लिए किया जाता है। डिजिटल सर्टिफिकेट, सर्टिफिकेट अथॉरिटी द्वारा जारी किए जाते हैं और ये सिक्योर सॉकेट लेयर (एसएसएल) प्रोटोकॉल के साथ उपयोग किए जाते हैं।
- **ई-कॉमर्स प्लेटफॉर्म:** ऐसा सॉफ्टवेयर जो एक ईकामर्स व्यवसाय चलाने के लिए आवश्यक विभिन्न प्रकार्य / कार्यप्रणालियाँ प्रदान करता है जैसे कि वेबसाइट, श्रेणी प्रबंधन, मूल्य निर्धारण प्रबंधन, आदेश प्रबंधन और भुगतान प्रबंधन। उदाहरण के लिए – शोपिफ़ाय, मैगनेटो और अन्य।
- **ईएमआई (समान मासिक किश्तें)**
  - बैंक द्वारा कार्डधारक (ग्राहक) को लेन-देन की राशि को मासिक आधार पर देय छोटी राशि में विभाजित करने का प्रावधान दिया गया है। इस सेवा के लिए बैंक द्वारा प्रोसेसिंग शुल्क या ब्याज वसूला जा सकता है।
- **ईएमवी** : यूरोपे, मास्टर कार्ड और वीजा, एक माइक्रोचिप-आधारित तकनीक है जिसे बिक्री के स्थान पर धोखाधड़ी को कम करने के लिए डिज़ाइन किया गया है।
- **एन्क्रिप्शन:** विशेष ज्ञान रखने वालों को छोड़कर किसी के लिए भी इसे अनुपयोगी बनाने के लिए प्रसंस्करण जानकारी को बदलने की प्रक्रिया को आमतौर पर एक कुंजी के रूप में संदर्भित किया जाता है।
- **समाप्ति तिथि:** वह तिथि जिस पर कार्ड की वैधता समाप्त हो जाती है। लेन-देन केवल उन कार्डों के लिए स्वीकृत किए जाएंगे जो अभी तक समाप्त नहीं हुए हैं।
- **फ्लैट शुल्क**: लेनदेन शुल्क प्रति लेनदेन है न कि लेनदेन राशि का प्रतिशत।
- **गिफ्ट कार्ड:** प्रीपेड/प्रीलोडेड मर्चेंट इंस्ट्रूमेंट जिसका उपयोग विशिष्ट व्यापारियों से खरीदारी के लिए किया जाता है।
- **गेटवे:** एक उद्यम जो एक डिजिटल वित्तीय सेवा प्रदाता के लिए विभिन्न कार्यों को आउट-सोर्स के आधार पर प्रबंधित करता है। इन कार्यों में लेनदेन प्रबंधन, ग्राहक डेटाबेस प्रबंधन और जोखिम प्रबंधन शामिल हो सकते हैं। प्रोसेसर भुगतान प्रणाली, योजनाओं, या स्विच की ओर से भी कार्य कर सकते हैं।

- **विनिमय शुल्क:** लेन-देन से संबंधित लागतों की भरपाई के लिए अधिग्रहणकर्ता द्वारा जारीकर्ता को भुगतान किया गया शुल्क। वीज़ा, मास्टरकार्ड और अन्य प्रदाता इंटरचेंज शुल्क दरों का निर्धारण करते हैं।
- **आईएमपीएस:** तत्काल भुगतान सेवाएं एनपीसीआई का एक उत्पाद है, जिसमें मोबाइल नंबर के आधार पर लाभार्थी को 1 लाख रुपये तक का तत्काल समय पर भुगतान किया जाता है।
- **अपने ग्राहक को जानें (केवाईसी):** व्यावसायिक संस्थाओं या व्यक्ति की जानकारी साबित करने वाली दस्तावेज़ का सेट।
- **मल्टी लेवल मार्केटिंग:** एक ऐसी प्रणाली जिसमें किसी कंपनी और साथ ही उनके द्वारा भर्ती किए गए किसी भी प्रतिभागी की ओर से वस्तु या सेवाओं को बेचने की प्रथा जिसके तहत प्रतिभागियों को उनकी बिक्री पर कमीशन प्राप्त होता है।
- **नियर फील्ड कम्युनिकेशन एनएफसी:** एनएफसी से लैस मोबाइल फोन से सक्षम टर्मिनल तक भुगतान डेटा संचारित करने के लिए भुगतान के भीतर उपयोग की जाने वाली संचार तकनीक।
- **एनईएफटी:** लाभार्थी को बैच वार भुगतान के लिए राष्ट्रीय इलेक्ट्रॉनिक फंड ट्रांसफर आरबीआई का एक भुगतान उत्पाद है।
- **वन टाइम पासवर्ड (ओटीपी):** ओटीपी या वन टाइम पासवर्ड एक अतिरिक्त सुरक्षा उपाय है जिसमें आपके ऑनलाइन लेनदेन के लिए दो-चरणीय प्रमाणीकरण शामिल है। यह समयबद्ध ओटीपी अधिकांश वित्तीय लेनदेन के लिए एक बहुत लोकप्रिय विकल्प बन गया है।
- **फ़िशिंग** - व्यक्तिगत जानकारी, जैसे पासवर्ड और क्रेडिट कार्ड नंबर प्राप्त करने के लिए व्यक्तियों को प्रेरित/प्रलोभित करने के लिए प्रतिष्ठित कंपनियों के नाम से ईमेल भेजने की धोखेबाज़ी की प्रथा।
- **पॉइंट ऑफ़ सेल डिवाइस टर्मिनल, स्वीकृति उपकरण, पीओएस, एमपीओएस:** ऐसा कोई भी उपकरण जो विशेष रूप से इलेक्ट्रॉनिक भुगतान की प्राप्ति के प्रबंधन के लिए है।
- **पीसीआई-डीएसएस:** ऐसी प्रथाएं जो उद्यम अंतिम उपयोगकर्ता डेटा की सुरक्षा के लिए करते हैं। "पीसीआई-डीएसएस" इसके लिए एक कार्ड उद्योग मानक है।
- **पी२पी; मूल्य का दूरस्थ सीमा-पार स्थानांतरण, सीमा-पार विप्रेषण:** दूसरे देश में किसी अन्य व्यक्ति को भुगतान करना और प्राप्त करना।
- **त्वरित प्रतिक्रिया कोड (क्यूआर)** - त्वरित प्रतिक्रिया (क्यूआर) कोड एक प्रकार का बारकोड है जो सूचनाओं को संग्रहीत करता है और एक डिजिटल डिवाइस, जैसे सेल फोन द्वारा पढ़ा जा सकता है।

- **समाधान**: समाधान एक लेखांकन प्रक्रिया है जिसमें आंकड़े सही हैं और मान्य किए जाने योग्य है यह सुनिश्चित करने के लिए रिकॉर्ड के दो सेट का उपयोग किया जाता है। इससे इस बात की पुष्टि की जाती है कि खाते से निकलने वाली राशि खर्च की गई राशि से मेल खाती है या नहीं और यह सुनिश्चित किया जाता है कि रिकॉर्डिंग अवधि के अंत में दोनों संतुलित हैं।
- **आवर्ती भुगतान:** ऐसे भुगतान जो हम आवधिक रूप में / समय-समय पर करते हैं, और आवधिकता साप्ताहिक, मासिक, त्रैमासिक, अर्ध-वार्षिक, वार्षिक हो सकती है उदाहरण: उपयोगिता बिल, बीमा प्रीमियम।
- **स्विच (राष्ट्रीय वित्तीय स्विच):** एक ऐसी संस्था जो एक प्रदाता से लेनदेन प्राप्त करती है और उन लेनदेन को दूसरे प्रदाता तक ले जाती है। स्विच द्वारा किसी योजना का स्वामित्व लिया जा सकता है या उसे किराए पर लिया जा सकता है या अलग-अलग प्रदाताओं द्वारा किराए पर लिया जा सकता है। अंतर-प्रतिभागी निपटान के लिए स्विच एक निपटान प्रणाली से जुड़ सकता है।
- **टीएटी** : टर्न अराउंड टाइम: किसी विशेष सेवा को वितरित करने के लिए प्रतिबद्ध समय (उदाहरण के लिए निपटान के लिए टीएटी टी +2 दिन है)।
- **यूनिफाइड पेमेंट इंटरफेस (यूपीआई):** यूपीआई भारत में डिजिटल भुगतान को बढ़ावा देने और इंटरऑपरेबिलिटी प्रदान करने के लिए एनपीसीआई द्वारा निर्मित एक डिजिटल भुगतान पहल है। एक बार जब ग्राहक बैंक के साथ यूपीआई के लिए पंजीकरण कर लेता है, तब वह एक अद्वितीय आभासी पहचानकर्ता बनाया जाता है और उसे भुगतान शुरू करने के लिए मोबाइल फोन से मैप किया जाता है, यूपीआई लाभार्थी की इस आभासी पहचान का प्रयोग करता है और रीयल-टाइम में पैसे ट्रांसफर करता है। यह सिंगल-क्लिक टू-फैक्टर ऑथेंटिकेशन पर काम करता है।
- **यूटीआर:** यूटीआर यूनिक ट्रांजैक्शन रेफरेंस नंबर है जो किसी भी ट्रांजैक्शन की विशिष्ट पहचान के लिए आईएमपीएस, एनईएफटी और आरटीजीएस सिस्टम में जेनरेट होता है। यूटीआर का प्रारूप पूर्वनिर्धारित होता है और लेन-देन शुरू करने वाले बैंक द्वारा तैयार/जनरेट किया जाता है।
- **बटुआ (वॉलेट) :** वॉलेट निधियों (फंड) रखने के लिए एक खाता है और इसका उपयोग विभिन्न खरीद के लिए किया जा सकता है। वॉलेट वर्चुअल हो सकता है जैसे कि मोबाइल वॉलेट (जैसे पेटीएम, फोनपे) अथवा फिजिकल हो सकता है (जैसे प्रीपेड कार्ड)।

****


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

OFFICE OF RBI OMBUDSMAN (MUMBAI-II)
MAHARASHTRA AND GOA

Design by M Muralidhar, Anupam Sharma